PCT / SE 2004 / 000945

REC'D 21 JUL 2004

WIPO PCT

PA 1185436

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

June 22, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/551,039*
FILING DATE: *March 09, 2004*

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

M. K. HAWKINS
Certifying Officer

PATENT APPLICATION SERIAL NO. ________________

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

03/11/2004 EAREGAY1 00000050 60551039

01 FC:1005 160.00 OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2001 — 481-697/59173

030904 13281 U.S. PTO

Mail Stop Provisional Patent Application

PTO/SB/16 (6-95)
Approved for use through 04/11/98. OMB 0651-0037
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53 (c).

	Docket Number	4147-66	Type a plus sign (+) inside this box→	+

INVENTOR(S)/APPLICANT(S)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
OYAMA	Johnson		Tokyo, Japan
KATO	Ryoji		Yokusuka Kanagawa, Japan

15535 U.S. PTO 60/551039

TITLE OF THE INVENTION (280 characters)

AAA SUPPORT FOR MOBILE IP

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ **Customer Number:** **23117**

Type Customer Number here

Place Customer Number Bar Label Here →

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification and Drawings — Number of Total Pages: 38

☐ Applicant claims "small entity" status.

☐ "Small entity" statement attached.

☐ Other (specify)

METHOD OF PAYMENT *(check one)*

☒ A check or money order is enclosed to cover the Provisional filing fees ($160.00)/($80.00)

☒ The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Account No. 14-1140. A duplicate copy of this sheet is attached.

PROVISIONAL FILING FEE AMOUNT ($): 160.00

The invention was made by an agency of the United States Government or under a contact with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,
SIGNATURE

DATE: March 9, 2004

TYPED or PRINTED NAME: John R. Lastova

REGISTRATION NO. *(if appropriate)*: 33,149

☐ Additional inventors are being named on separately numbered sheets attached hereto.

PROVISIONAL APPLICATION FILING ONLY

824726

Atty. Dkt. 4147-66
PE19316US00

U.S. PROVISIONAL PATENT APPLICATION

Inventor(s): Johnson OYAMA
Ryoji KATO

Invention: AAA SUPPORT FOR MOBILE IP

NIXON & VANDERHYE P.C.
ATTORNEYS AT LAW
1100 NORTH GLEBE ROAD, 8TH FLOOR
ARLINGTON, VIRGINIA 22201-4714
(703) 816-4000
Facsimile (703) 816-4100

824713

AAA SUPPORT FOR MOBILE IP

TECHNICAL FIELD OF THE INVENTION

The present invention generally relates to mobile communications, and in particular to AAA support for mobile IP (Internet Protocol), specifically authentication and/or authorization.

BACKGROUND OF THE INVENTION

Mobile IP (MIP) defines a method that allows a Mobile Node (MN) to change its point of attachment to the Internet with minimal service disruption. MIP in itself does not provide any specific support for mobility across different administrative domains, which limits the applicability of MIP in a large-scale commercial deployment.

AAA (Authorisation, Authentication, Accounting) protocols such as the Diameter protocol precisely enable mobile users to roam and obtain service in networks that may not necessarily be owned by their home service provider. For MIP to be deployed in commercial networks, there therefore has to be AAA support for the protocol. The general architecture for MIP AAA is illustrated in Fig. 1.

For the case of Mobile IPv6 (MIPv6) [1], an Internet draft [2] has been proposed which specifies a new application to Diameter that enables MIPv6 roaming in networks other than the home domain network. Very recently, an Internet draft [3], which defines an architecture and related protocols for performing dynamic Mobile IPv6 authorization and configuration relaying on an AAA infrastructure, has been published. In this draft, the necessary interaction between the AAA server of the home provider and the mobile node is realized using EAP (Extensible Authentication Protocol), exploiting the capability of some EAP methods to convey generic information items together with authentication data. This approach has the advantage

that the access equipment acts just as a pass-through for EAP messages and therefore does not play any active role in the Mobile IPv6 negotiation procedure, which makes the solution easier to deploy and maintain. The Internet draft [4] defines the Command-Codes and APVs necessary to carry EAP packets between a Network Access Server (NAS) and a back-end authentication server.

Fig. 2 schematically illustrates an exemplary HMIPv6 domain. Hierarchical mobility management for Mobile IPv6 reduces the amount of signaling between the MN, its Correspondent Nodes (CN), and its HA by using a Mobility Anchor Point (MAP) located in the visited network, which improves the performance of Mobile IPv6 in terms of handoff speed [5]. An MN entering a MAP domain will receive Router Advertisements containing information on one or more local MAPs. The MN can bind its current location (on-link Care of Address or LCoA) with an address on the MAP's subnet called Regional Care of Address (RCoA). Acting as a local HA, the MAP will receive all packets on behalf of the MN it is serving and will encapsulate and forward them directly to the MN's LCoA.

HMIPv6 itself, as in the MIP case, does not provide any specific support for mobility across different administrative domains, which limits the applicability of HMIPv6 in a large-scale commercial deployment.

It can normally be expected that the MN would need to be authenticated first before being authorized to use the services of HMIP. It is crucial that the security relationship between the mobile node and the MAP is of strong nature; it must involve mutual authentication, integrity protection and protection against replay attacks. To this end, distribution of security keys between MN and MAP currently bas to rely on Public Key Infrastructures (PKI) and complex protocols. The current HMIP draft [5] also limits the location of the MAP to the visited network.

THE INVENTION

It has been recognized that there are cases where it would be beneficial to have MAP located in the home network or other networks, such as for the case where the visited network does not provide MAP support. A MAP located in the home network can be used to address the HA scalability issues, offloading the HA by reducing the number of binding updates that go to the HA during intra-MAP domain mobility. By selecting the MAP to be topographically close to the location of the MN, fast handovers can be realized. An example of MAP located in the home network is illustrated in Fig. 3.

Among other things, the invention proposes solutions for AAA support for HMIPv6, and specifically authentication and/or authorization support. For example, a "Diameter HMIPv6 Application" is created which carries HMIPv6 related information facilitating discovery of MAP, dynamic allocation of MAP, dynamic allocation of RCoA, distribution of security keys between MN and MAP, and possible piggyback of HMIPv6 mobility procedures. Also, as a possible complement and/or alternative to the Diameter HMIPv6 Application, a new EAP authentication protocol "HMIPv6 authentication method" or "EAP/HMIPv6" is defined that can carry the above HMIPv6 related information – a suitable EAP carrier such as the Diameter EAP Application can then transport EAP/HMIPv6 within the AAA infrastructure. Furthermore with AAA support for HMIPv6, additional scenarios where MAP is located in the home network or other network than the visited become a possibility.

In the following, exemplary aspects of the invention will be described, including preferred features as well as optional features.

(1) A novel architecture for HMIPv6 AAA, as illustrated in Fig. 4.

(2) A new EAP authentication protocol "HMIPv6 authentication method" or "EAP/HMIPv6" is defined that carries HMIPv6 related information facilitating

for example discovery of MAP, dynamic allocation of MAP, dynamic allocation of RCoA, distribution of security keys between MN and MAP, and possible piggyback of HMIPv6 mobility procedures. A suitable EAP carrier such as the Diameter EAP Application can then transport EAP/HMIPv6 within the AAA infrastructure.

EAP/HMIPv6 is a superset of EAP/MIPv6 which is described in detail in Appendix A, and defines in addition, new HMIP-specific Type-Length-Values (TLV's). By including the TLV's of EAP/MIPv6 as part of EAP/HMIPv6, it will be possible to accommodate simultaneous executions of both MIPv6 and HMIPv6 authentication and/or authorization in a single traversal which enables shorter setup times. It would also be possible to execute only HMIPv6 authentication and/or authorization without the MIPv6 counterpart and vice versa, depending on the particular need of the MN at a specific instance. This allows a single EAP authentication protocol, EAP/HMIPv6, to be flexibly used on various use case scenarios.

The use of EAP allows the AAA Client (and AAAv) to be agnostic to HMIP procedures (i.e., this removes dependency on HMIP support of the visited network), and act as mere pass-through agent(s), which is one of the major advantages of using EAP.

Furthermore, piggyback of HMIPv6 mobility procedures in EAP/HMIPv6 allow possible shortening of overall setup times by optimizing authentication, authorization, and mobility in a common procedure.

(3) A "Diameter HMIPv6 Application" is created which carries HMIPv6 related information facilitating for example discovery of MAP, dynamic allocation of MAP, dynamic allocation of RCoA, distribution of security keys between MN and MAP, and possible piggyback of HMIPv6 mobility procedures.

The Diameter HMIPv6 Application is a superset of the Diameter MIPv6 Application described in [2], and defines in addition, new HMIP-specific command codes, AVP's, and/or flags. By including the command codes, AVP's, and flags of the Diameter MIPv6 Application as part of the Diameter HMIPv6 Application, it will be possible to accommodate simultaneous executions of both MIPv6 and HMIPv6 authentication and/or authorization in a single traversal which enables shorter setup times. It would also be possible to execute only HMIPv6 authentication and/or authorization without the MIPv6 counterpart and vice versa, depending on the particular need of the MN at a specific instance. This allows a single application, the Diameter HMIPv6 Application, to be flexibly used on various use case scenarios.

Furthermore, piggyback of HMIPv6 mobility procedures in Diameter HMIPv6 Application allows possible shortening of overall setup times by optimizing authentication, authorization, and mobility in a common procedure.

(4) The location of MAP can be in the home network, visited network, or other networks. There is no longer mandatory dependency on the Router Advertisements containing information on MAPs within pre-defined MAP domains. Technically, it would be possible for the MN to bind with any MAP as long as an RCoA on the MAP can be obtained with AAA support, if operators allow this.

(5) Reassignment of MAP may occur during the following cases:

- Expiration of security keys between MN and MAP – for this case, the MN initiates HMIPv6 re-authentication / authorization, and the network may assign a different MAP that is more appropriate based on, e.g., current topological location of MN

- At the request of MN (MN initiated) – for this case, the MN initiates HMIPv6 re-authentication / authorization requesting for reassignment of MAP

- At the request of the network (network initiated) – for the case, either the AAAh or AAAv initiates the reassignment of MAP and "pushes" this to the MN when the need arises, e.g., when the MN moves to an AR that is better covered by a new MAP.

(6) The possible different protocol combinations between the segments AAA Client – AAAh, and AAAh – (AAAv) – MAP are summarized below:

	AAA Client <-> AAAh	AAAh <-> (AAAv) <-> MAP
(i)	Diameter HMIPv6 Application	Diameter HMIPv6 Application
(ii)	Diameter/EAP/HMIPv6	Diameter HMIPv6 Application
(iii)	Diameter/EAP/HMIPv6	Diameter/EAP/HMIPv6

Note: (iii) is applicable for the case where the MAP is located in the home network.

Where MAP is located in the visited network, the AAAv may be involved in the selection of MAP based on visited network policy.

EAP/HMIPv6 Protocol Details

In the following, details of an exemplary EAP/HMIPv6 protocol are defined. New

EAP TLV's are defined that would carry information that facilitate for example discovery of MAP, dynamic allocation of MAP, dynamic allocation of RCoA, distribution of security keys between MN and MAP, and possible piggyback of HMIPv6 mobility procedures. The TLV's of EAP/MIPv6 are also part of EAP/HMIPv6.

An exemplary summary matrix of EAP/HMIPv6 TLV's is given below in Table I:

EAP/HMIPv6 Type-Length-Values	Source	Destination	Purpose	Comment
HMIPv6 specific TLV's:				
• RCoA Request EAP-TLV attribute	MN	AAAh	request RCoA	
• RCoA Response EAP-TLV attribute	AAAh	MN	assign RCoA	MAP in home
	AAAh	MN	forward RCoA from AAAv	MAP in visited
RCoA EAP-TLV attribute	AAAh	MAP	assign RCoA	MAP in home
• MAP Address Request EAP-TLV attribute	MN	AAAh	request MAP address	
• MAP Address Response EAP-TLV attribute	AAAh	MN	assign MAP address	MAP in home
	AAAh	MN	forward MAP address from AAAv	MAP in visited
MAP-MN Pre-shared Key Generation Nonce EAP-TLV attribute	MN	AAAh	seed for MN-MAP key	
• MAP-MN Pre-shared Key EAP-TLV attribute	AAAh	MAP	assign MN-MAP key	MAP in home
• MAP IKE KeyID EAP-TLV attribute	AAAh	MN	assign IKE KeyID	MAP in home
• MAP-MN IPSec SPI EAP-TLV attribute	MAP	MN via AAAh	assign SPI	MAP in home
	AAAh	MN	forward from MAP	MAP in visited
• MAP-MN IPSec Protocol EAP-TLV attribute	MAP	MN via AAAh	assign IPSec Protocol	MAP in home
	AAAh	MN	forward from MAP	MAP in visited
• MAP-MN IPSec Crypto EAP-TLV attribute	MAP	MN via AAAh	assign IPSec Crypto	MAP in home
	AAAh	MN	forward from MAP	MAP in visited
• MAP-MN IPSec Key Lifetime EAP-TLV attribute	MAP	MN via AAAh	assign IPSec Key Lifetime	MAP in home
	AAAh	MN	forward from MAP	MAP in visited
• HMIP-Binding-Update EAP-TLV attribute	MN	MAP via AAAh	piggyback HMIP binding update	MAP in home
	MN	AAAh	piggyback HMIP binding update	MAP in visited
• HMIP-Binding-Acknowledgement EAP-TLV attribute	MAP	MN via AAAh	piggyback HMIP binding ack.	MAP in home
	AAAh	MN	forward from MAP	MAP in visited
New MIPv6 specific TLV's (proposed improvements to EAP/MIPv6 TLV set):				
• MIPv6 Home Address EAP-TLV attribute	AAAh	HA	assign MN Home Address	
• HA-MN Pre-shared Key EAP-TLV attribute	AAAh	HA	assign HA-MN key	
HA-MN IPSec Protocol EAP-TLV attribute	HA	MN via AAAh	assign IPSec Protocol	
• HA-MN IPSec Crypto EAP-TLV attribute	HA	MN via AAAh	assign IPSec Crypto	
• MIP-Binding-Update EAP-TLV attribute	MN	HA via AAAh	piggyback MIP binding update	
• MIP-Binding-Acknowledgement EAP-TLV attribute	HA	MN via AAAh	piggyback MIP binding ack.	
Existing EAP/MIPv6 TLV's (EAP/MIPv6):				
• MD5 Challenge EAP-TLV attribute	AAAh	MN	issue challenge	
• MD5 Response EAP-TLV attribute	MN	AAAh	provide response to challenge	
• MIPv6 Home Address Request EAP-TLV attribute	MN	AAAh	request MN home address	
• MIPv6 Home Address Response EAP-TLV attribute	AAAh	MN	assign MN home address	
• MIPv6 Home Agent Address Request EAP-TLV attribute	MN	AAAh	request HA address	
• MIPv6 Home Agent Address Response EAP-TLV attribute	AAAh	MN	assign HA address	
• HA-MN Pre-shared Key Generation Nonce EAP-TLV attribute	MN	AAAh	seed for HA-MN key	
• IKE KeyID EAP-TLV attribute	AAAh	MN	info for obtaining HA-MN pre-shared key from AAAh	
• HA-MN IPSec SPI EAP-TLV attribute	HA	MN via AAAh	assign SPI	
• HA-MN IPSec Key Lifetime EAP-TLV attribute	HA	MN via AAAh	assign IP Sec Key lifetime	
• PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute	MN	AAAh	seed for PAC-PAA key	

Note: the IKE KeyID includes some octets which informs the HA/MAP how to retrieve (or generate) the HA-MN pre-shared key/MAP-MN pre-shared key from AAAh.

Figs. 5 and 6 show exemplary general signaling flows for HMIPv6 AAA using Diameter/EAP/HMIPv6 (simultaneous MIPv6 + HMIPv6 initiation requests). In particular, Fig. 5 illustrates Diameter/EAP/HMIPv6 signaling flow for the MAP in home network case. Fig. 6 illustrates Diameter/EAP/HMIPv6 signaling flow for the MAP in visited network case (Diameter HMIPv6 Application is used between AAAh and MAP).

Diameter HMIPv6 Application Protocol Details

Details of the Diameter HMIPv6 Application protocol are defined below. New HMIP-specific command codes, AVP's, and/or flags are defined that would carry information that facilitate for example discovery of MAP, dynamic allocation of MAP, dynamic allocation of RCoA, distribution of security keys between MN and MAP, and possible piggyback of HMIPv6 mobility procedures. The command codes, AVP's, and flags of the Diameter MIPv6 Application are also part of the Diameter HMIPv6 Application.

An exemplary summary matrix of Diameter HMIPv6 Application Command Codes and AVP's is given below in Table 2:

Diameter HMIPv6 Application Command Codes and AVP's	Source	Destination	Purpose	Comment
HMIPv6 specific command codes MAP-HMIPv6-Request Command (MAR) MAP-HMIPv6-Answer Command (MAA)	AAAh AAAh MAP MAP	MAP MAP via AAAv AAAh AAAh via AAAv	exchange of HMIP AVP's exchange of HMIP AVP's exchange of HMIP AVP's exchange of HMIP AVP's	MAP in home MAP in visited MAP in home MAP in visited
HMIPv6 specific AVP's HMIP-Binding-Update AVP HMIP-Binding-acknowledgement AVP RCoA AVP MAP Address AVP HMIPv6-Feature-Vector AVP MAP-Requested Flag			HMIP Binding Update message sent by MN to MAP HMIP Binding Acknowledgement sent by MAP to MN RCoA MAP address requests for a dynamic MAP assignment	
Existing Diameter MIPv6 Application command codes AA-Registration-Request Command (ARR) AA-Registration-Answer Command(ARA) Home-Agent-MIPv6-Request Command (HOR) Home-Agent-MIPv6-Answer Command (HOA)	AAA Client AAAh AAAh HA	AAAh (via AAAv) AAA Client (via AAAv) HA AAAh		
Existing Diameter MIPv6 Application AVP's MIP-Binding-Update AVP MIP-Binding-acknowledgement AVP MIPv6-Mobile-Node-Address AVP MIPv6-Home-Agent-Address AVP MIPv6-Feature-Vector AVP Home-Agent-Requested Flag			Mobile IP Binding Update message sent by MN to HA Mobile IP Binding Acknowledgement sent by HA to MN the Mobile Node's Home Address the Mobile Node's Home Agent Address requests for a dynamic home agent assignment	

Figs. 7 and 8 show exemplary general signaling flows for HMIPv6 AAA using Diameter HMIPv6 Application (simultaneous MIPv6 + HMIPv6 initiation requests). In particular, Fig. 7 illustrates Diameter HMIPv6 Application signaling flow for the MAP in home network case. Fig. 8 illustrates Diameter HMIPv6 Application signaling flow for the MAP in visited network case.

Among other application areas, the invention is applicable to all access networks such as WLAN, CDMA2000, WCDMA and so forth, where MIPv6/HMIPv& can be used, including technologies such as AAA and IPv6 mobility, systems such as CMS11, WCDMA and GSM systems, sub-systems such as service/application subsystems and terminals, and products such as AAA servers, Home Agent Servers and terminal nodes.

The embodiments described above are merely given as examples, and it should be

understood that the present invention is not limited thereto. Further modifications, changes and improvements which retain the basic underlying principles disclosed herein are within the scope of the invention.

REFERENCES

[1] Mobility Support in IPv6, D. Johnson, C. Perkins, J. Arkko, June 30, 2003, <draft-ietf-mobileip-ipv6-24.txt>.

[2] Diameter Mobile IPv6 Application, Stefano M. Faccin, Franck Le, Basavaraj Patil, Charles E. Perkins, April 2003, <draft-le-aaa-diameter-mobileipv6-03.txt>.

[3] MIPv6 Authorization and Configuration based on EAP, G. Giaretta, I. Guardini, E. Demaria, February 2004, <draft-giaretta-mip6-authorization-eap-00.txt>.

[4] Diameter Extensible Authentication Protocol (EAP) Application, P. Eronen, T. Hiller, G. Zorn, February 16, 2004, <draft-ietf-aaa-eap-04.txt>.

[5] Hierarchical Mobile IPv6 mobility management (HMIPv6), Hesham Soliman, Claude Castelluccia, Karim El-Malki, Ludovic Bellier, June, 2003, <draft-ietf-mobileip-hmipv6-08.txt>.

ABBREVIATIONS

AAA - Authentication Authorisation and Accounting
AAAh - Home AAA Server
AAAv - Visited AAA Server
AR - Access Router
ARA - AA-Registration-Answer Command
ARR - AA-Registration-Request Command
AVP - Attribute-Value Pair
CN - Correspondent Node
EAP - Extensible Authentication Protocol
HA - Home Agent
HMIPv6 - Hierarchical Mobile IP version 6
HOA - Home-Agent-MIPv6-Answer Command
HOR - Home-Agent-MIPv6-Request Command
ICMP - Internet Control Message Protocol
IKE - Internet Key Exchange
IPsec - IP Security
LCoA - on-Link Care of Address
MAP - Mobility Anchor Point
MD5 - Message Digest 5
MIP - Mobile IP
MIPv6 - Mobile IP version 6
MN - Mobile Node
PANA - Protocol for Carrying Authentication for Network Access
PKI - Public Key Infrastructure
RA - Router Advertisement
RCoA - Regional Care of Address
TLV - Type-Length-Value

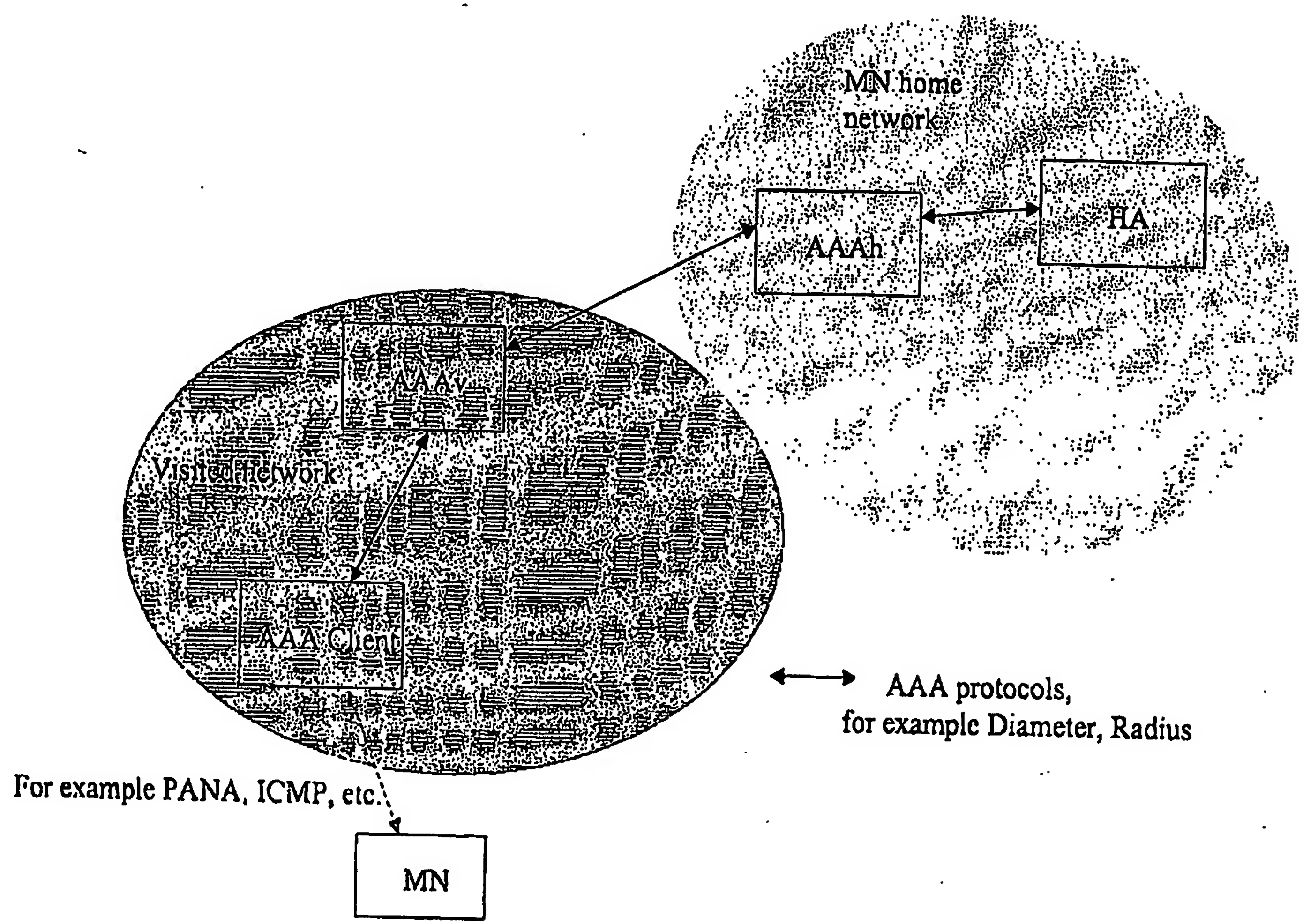
MN home network
HA
AAAh
AAAv
Visited network
AAA Client
MN
For example PANA, ICMP, etc.
AAA protocols, for example Diameter, Radius

Fig. 1

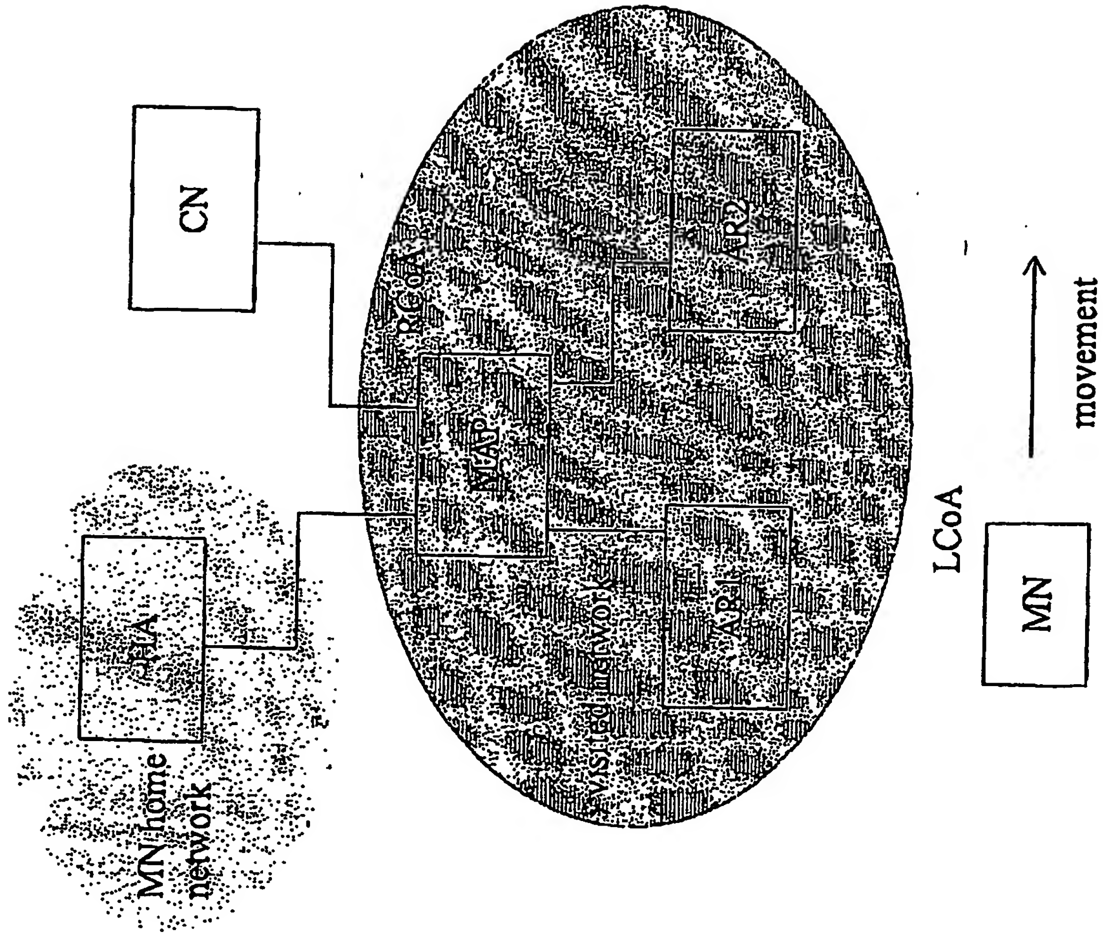
CN
RCoA
MAP
AR2
AR1
visited network
HA
MN home network
LCoA
MN
movement

Fig. 2

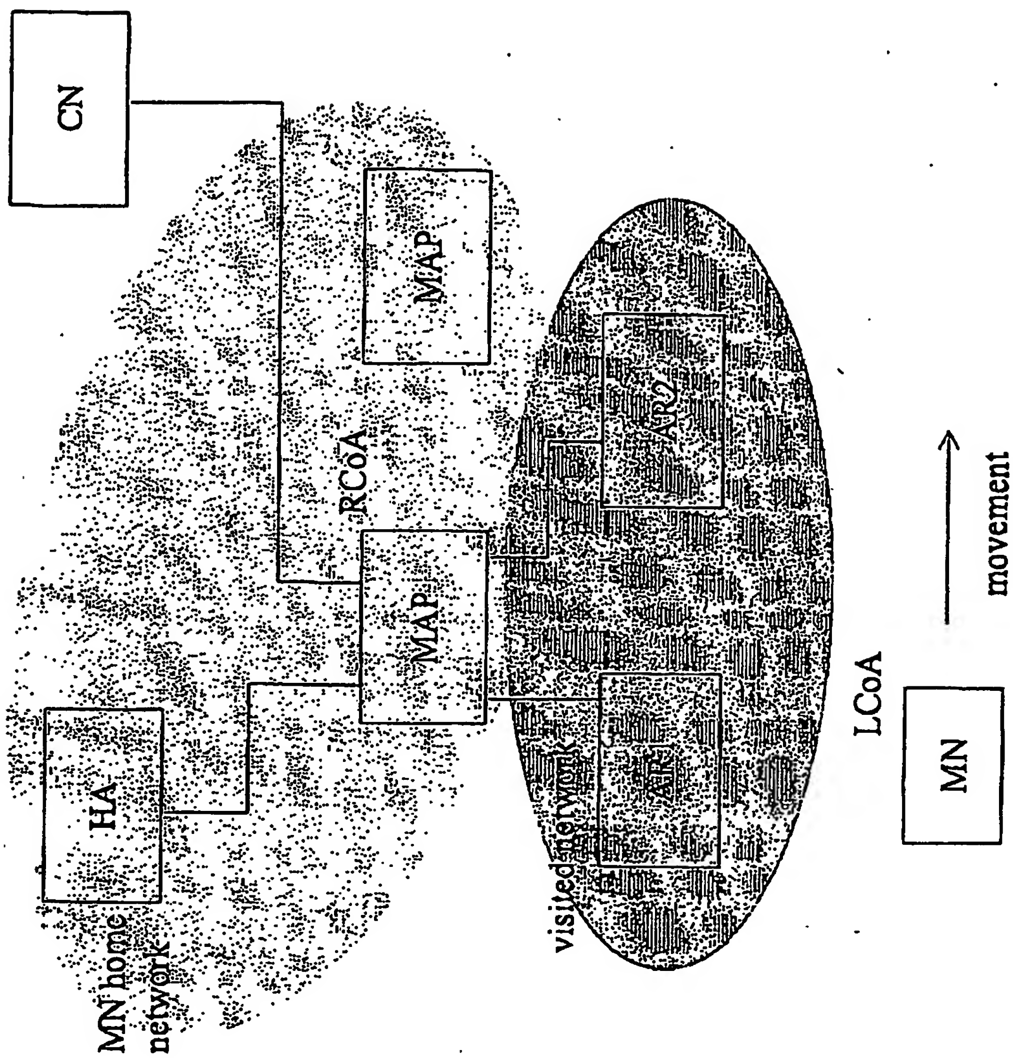
CN
MAP
RCoA
MAP
HA
MN home network
visited network
LCoA
MN
movement

Fig. 3

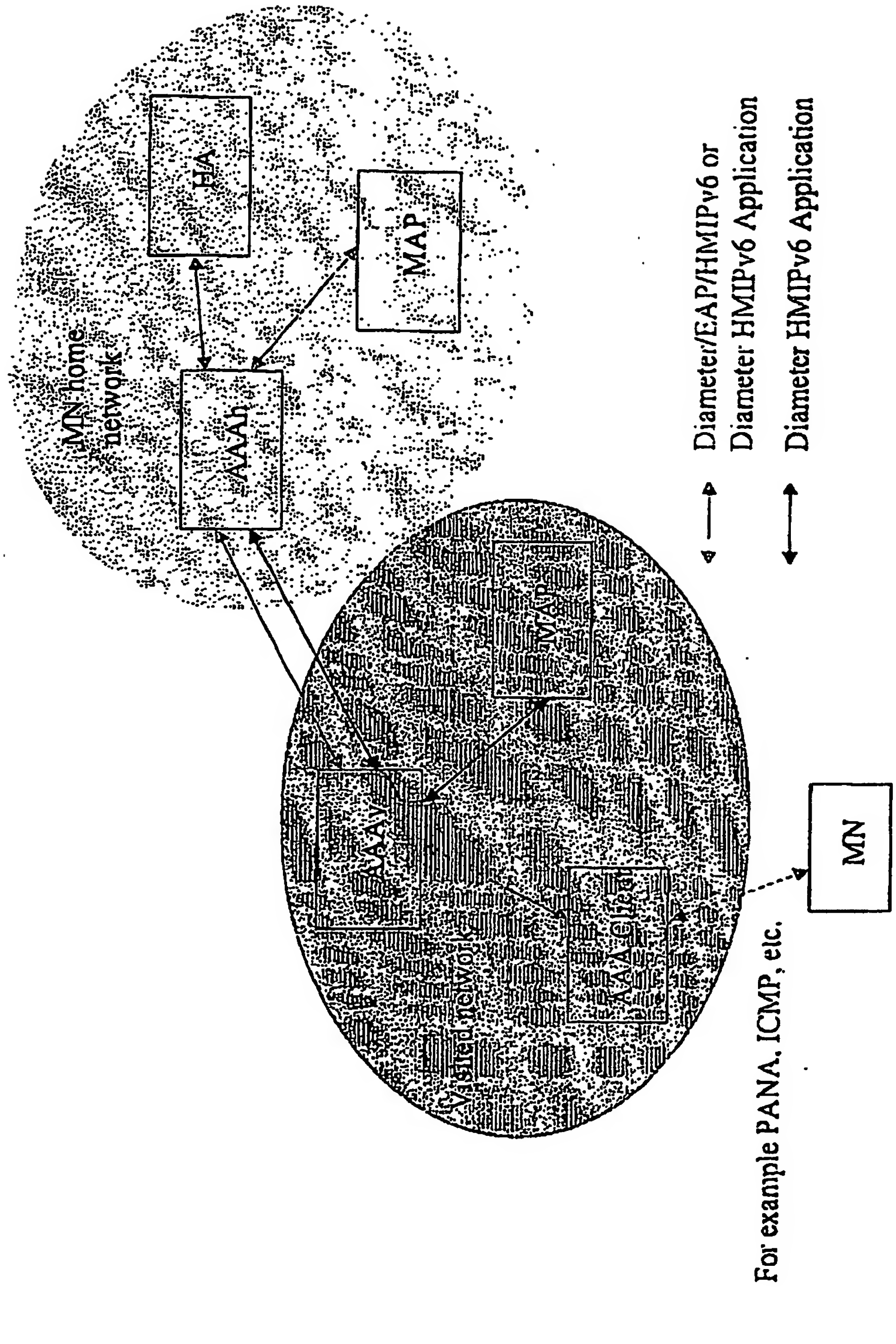
MN home network
HA
MAP
AAAh
Visited network
MAP
AAAv
AAAclient
MN
For example PANA, ICMP, etc.
Diameter/EAP/HMIPv6 or Diameter HMIPv6 Application
Diameter HMIPv6 Application

Fig. 4

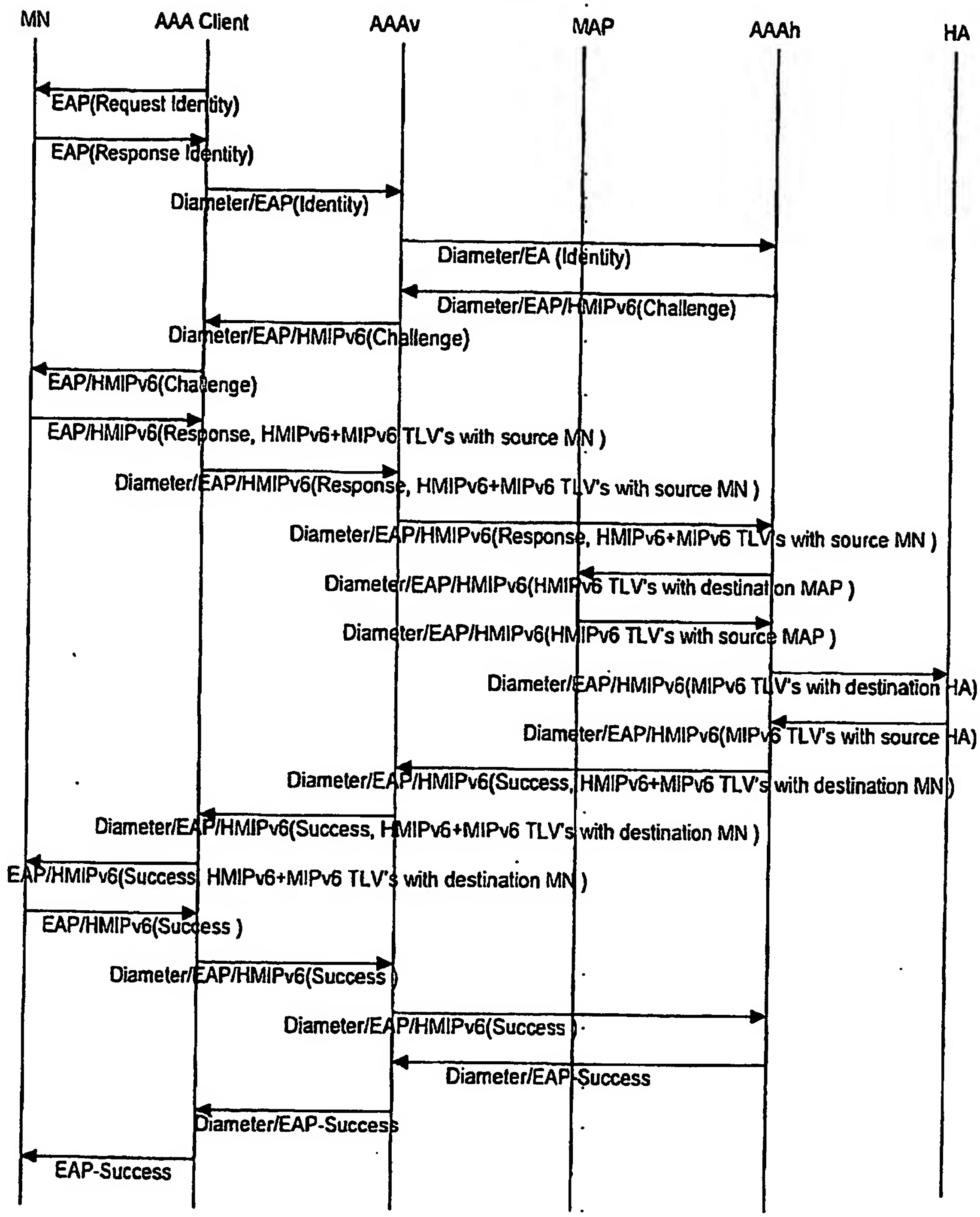
MN
AAA Client
AAAv
MAP
AAAh
HA
EAP(Request Identity)
EAP(Response Identity)
Diameter/EAP(Identity)
Diameter/EA (Identity)
Diameter/EAP/HMIPv6(Challenge)
Diameter/EAP/HMIPv6(Challenge)
EAP/HMIPv6(Challenge)
EAP/HMIPv6(Response, HMIPv6+MIPv6 TLV's with source MN)
Diameter/EAP/HMIPv6(Response, HMIPv6+MIPv6 TLV's with source MN)
Diameter/EAP/HMIPv6(Response, HMIPv6+MIPv6 TLV's with source MN)
Diameter/EAP/HMIPv6(HMIPv6 TLV's with destination MAP)
Diameter/EAP/HMIPv6(HMIPv6 TLV's with source MAP)
Diameter/EAP/HMIPv6(MIPv6 TLV's with destination HA)
Diameter/EAP/HMIPv6(MIPv6 TLV's with source HA)
Diameter/EAP/HMIPv6(Success, HMIPv6+MIPv6 TLV's with destination MN)
Diameter/EAP/HMIPv6(Success, HMIPv6+MIPv6 TLV's with destination MN)
EAP/HMIPv6(Success, HMIPv6+MIPv6 TLV's with destination MN)
EAP/HMIPv6(Success)
Diameter/EAP/HMIPv6(Success)
Diameter/EAP/HMIPv6(Success)
Diameter/EAP-Success
Diameter/EAP-Success
EAP-Success

Fig. 5

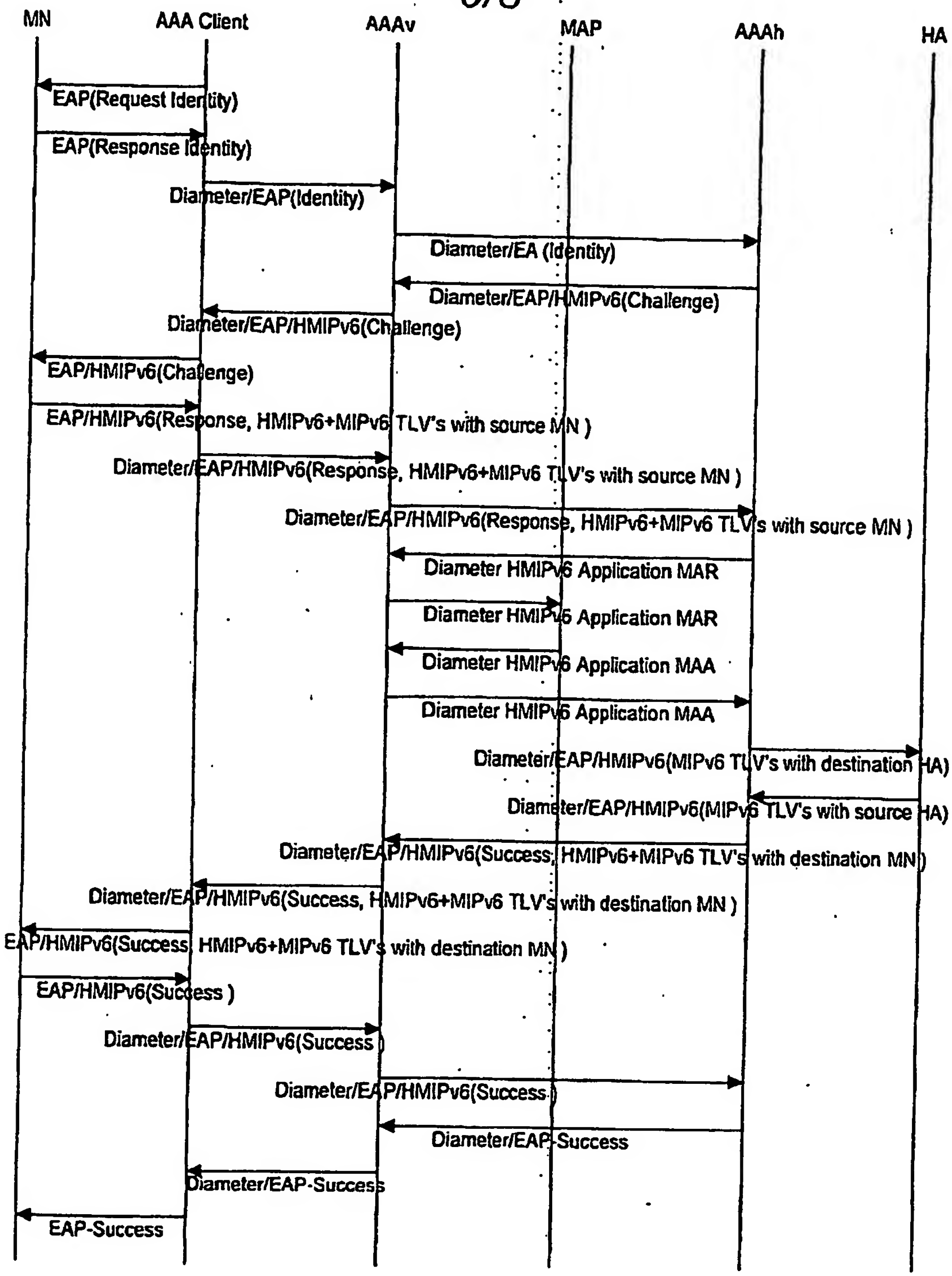
MN
AAA Client
AAAv
MAP
AAAh
HA
EAP(Request Identity)
EAP(Response Identity)
Diameter/EAP(Identity)
Diameter/EA (Identity)
Diameter/EAP/HMIPv6(Challenge)
Diameter/EAP/HMIPv6(Challenge)
EAP/HMIPv6(Challenge)
EAP/HMIPv6(Response, HMIPv6+MIPv6 TLV's with source MN)
Diameter/EAP/HMIPv6(Response, HMIPv6+MIPv6 TLV's with source MN)
Diameter/EAP/HMIPv6(Response, HMIPv6+MIPv6 TLV's with source MN)
Diameter HMIPv6 Application MAR
Diameter HMIPv6 Application MAR
Diameter HMIPv6 Application MAA
Diameter HMIPv6 Application MAA
Diameter/EAP/HMIPv6(MIPv6 TLV's with destination HA)
Diameter/EAP/HMIPv6(MIPv6 TLV's with source HA)
Diameter/EAP/HMIPv6(Success, HMIPv6+MIPv6 TLV's with destination MN)
Diameter/EAP/HMIPv6(Success, HMIPv6+MIPv6 TLV's with destination MN)
EAP/HMIPv6(Success, HMIPv6+MIPv6 TLV's with destination MN)
EAP/HMIPv6(Success)
Diameter/EAP/HMIPv6(Success)
Diameter/EAP/HMIPv6(Success)
Diameter/EAP-Success
Diameter/EAP-Success
EAP-Success

Fig. 6

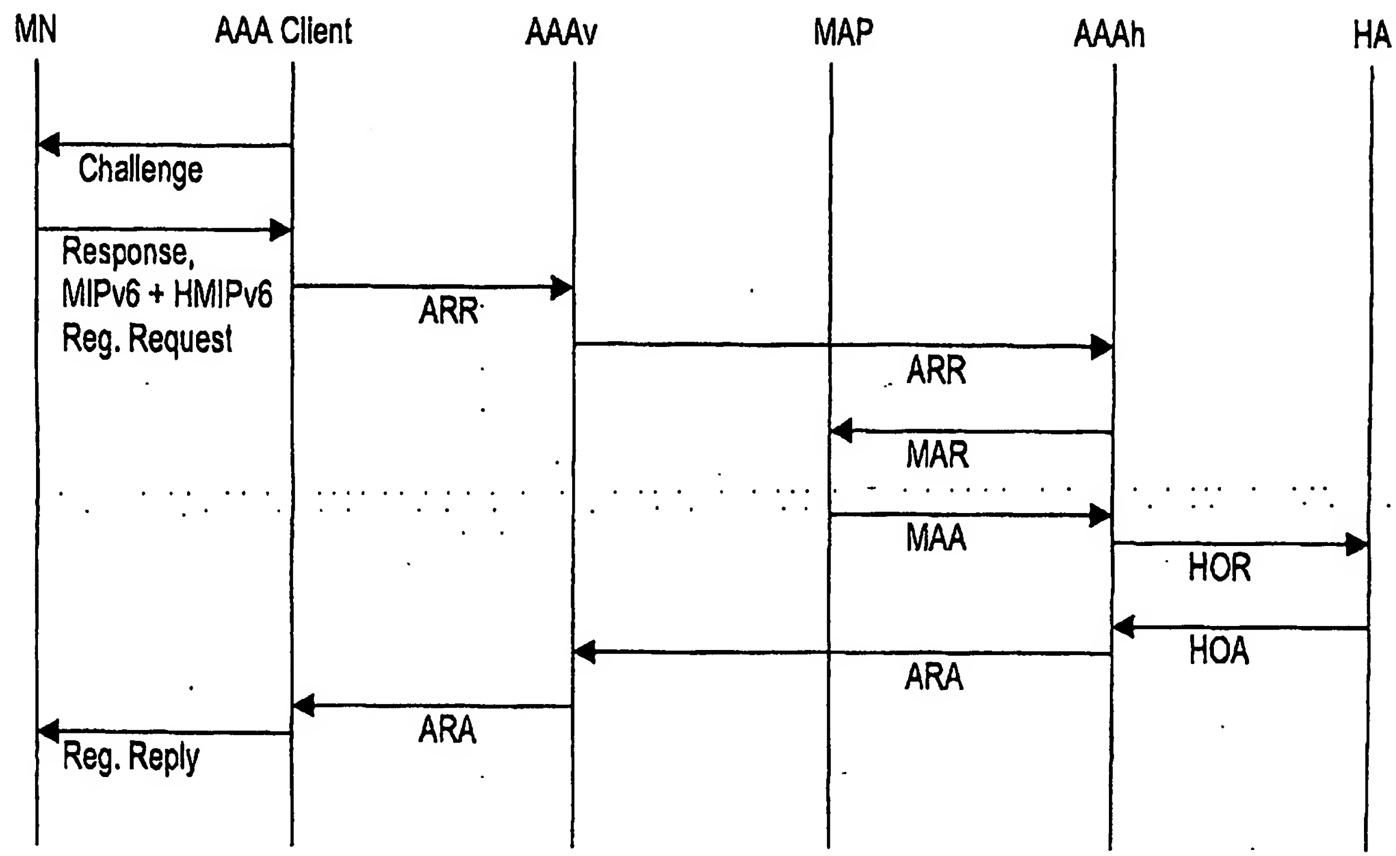
MN
AAA Client
AAAv
MAP
AAAh
HA
Challenge
Response,
MIPv6 + HMIPv6
Reg. Request
ARR
ARR
MAR
MAA
HOR
HOA
ARA
ARA
Reg. Reply

Fig. 7

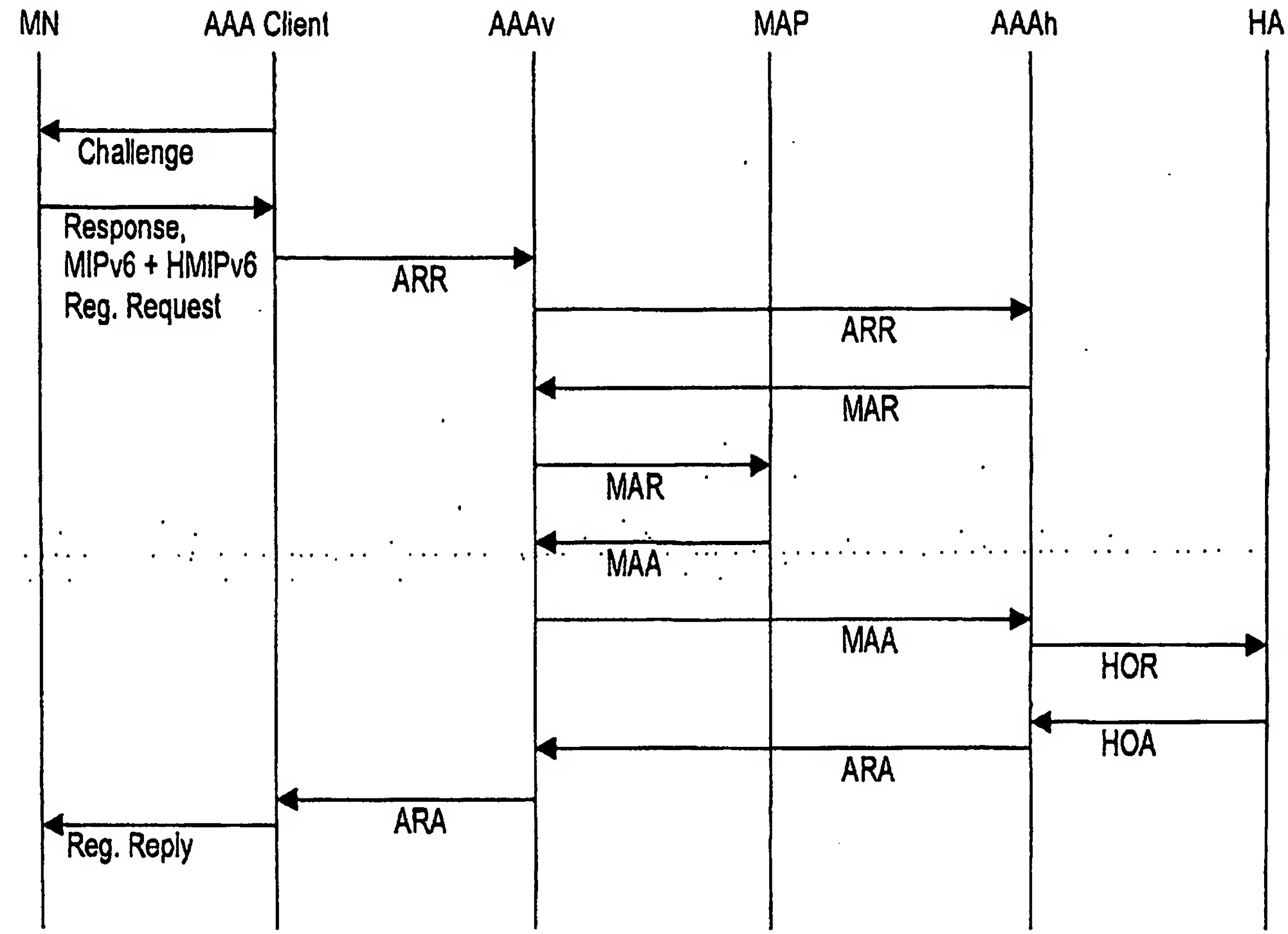
MN
AAA Client
AAAv
MAP
AAAh
HA
Challenge
Response,
MIPv6 + HMIPv6
Reg. Request
ARR
ARR
MAR
MAR
MAA
MAA
HOR
HOA
ARA
ARA
Reg. Reply

Fig. 8

APPENDIX A

Mobile IPv6 (MIPv6) capable mobile nodes, such as cellular phones, laptops and other end-user equipment, can roam between networks that belong to their home service provider as well as others. Roaming in foreign networks is enabled as a result of the service level and roaming agreements that exist between operators. One of the key AAA protocols that contribute to making this kind of a roaming mechanism possible is Diameter and the general architecture for MIPv6 AAA is schematically illustrated in Fig. 1.

Finding a well-functioning and complete MIPv6 AAA solution combining mobility with authentication/security for mobile communication would be very desirable. For instance, AAA can then be used to check/control who is entering the network. However, in the prior art only partial solutions are presented. These are generally non-consistent with each other and do not work end to end.

In [4], for example, attempts are made to specify a new application to Diameter enabling Mobile IPv6 roaming in networks other than the home domain. The Internet draft identifies information that typically needs to be exchanged between a MN and an AAA Client in the network and suggests use of the new Diameter application in exchanges of this information between AAA Client and AAAv, between AAAv and AAAh, and between HA and the AAA infrastructure. However, no particular mechanism to convey information between the mobile node and the AAA Client is specified. This, together with other shortcomings, makes this solution unsatisfactory and non-complete.

Thus, the need for an appropriate mechanism for MIPv6 AAA remains.

It is desirable to provide a complete mechanism for combining terminal mobility and user authentication in networks with mobile nodes, and to enable MIPv6 AAA.

This is achieved by means of a new EAP authentication protocol referred to as "EAP/MIPv6" (or "MIPv6 authentication method"). Preferably, the invention enables MIPv6 AAA by using a combination of PANA and Diameter as carrier protocols. The EAP/MIPv6 protocol can carry information that facilitates MIPv6 authentication, as well as dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security.

PANA is preferably used in carrying EAP/MIPv6 between MN/PAC and PAA/AAA Client. There are alternative carrier protocols, though. Diameter EAP Application [3] is generally used to transport EAP/MIPv6 between PAA/AAA Client and AAAv, and between AAAv and AAAh. The Diameter protocol is also used by AAAh for assignment to PAA/EP of security keys for PANA security, optional MIP packet filters via MIP filter rules, and optional QoS parameters etc. However, there may be embodiments using another suitable AAA protocol, such as Radius, instead of Diameter.

The exchanges between HA and the AAA infrastructure may for instance follow the AAAh-HA interface protocol specified in Diameter MIPv4 Application [2], or alternatively employ a mechanism similar to that currently used in 3GPP2 (i.e. [9]) in conjunction with the IKE [8] framework.

MIPv6 handoffs use a subset of the procedures used for MIPv6 initiation. For the handoff case, EAP/MIPv6 would only need to carry information that facilitates MIPv6 authentication, and distribution of security keys between PAC and PAA for PANA security.

For the case where EAP is used for WLAN authentication, e.g., EAP/AKA, PANA can be used for transporting EAP/AKA between PAC and PAA for WLAN access authentication instead of [10]. By carrying multiple EAP sequences in a single PANA

sequence, both EAP/AKA authentication of WLAN and EAP/MIPv6 can take place within a single PANA sequence for optimization purpose.

According to the authentication method of the invention, new EAP TLVs are defined for carrying MIPv6 authentication information. In case MD5 challenge authentication is used, these typically includes a MD5 Challenge attribute and a MD5 Response EAP-TLV attribute.

The authentication protocol preferably defines a number of additional EAP TLVs for dynamic MN home address allocation, dynamic HA allocation and distribution of security keys between HA and MN. These attributes are optional and there may be implementations lacking some or all of them. Furthermore, for distribution of security keys between PAC and PAA for PANA security, a PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute is generally needed.

By means of the attributes like these, the EAP protocol is allowed to carry MIPv6-related auxiliary information, such as requests for dynamic MN home address allocation, dynamic Home Agent allocation, as well as nonces/seeds for creation of necessary security keys, in addition to the main IPv6 authentication information. This is a major advantage of the invention.

Introductory discussion

As mentioned in the background section, a proposal which attempts to specify a new application to Diameter that enables Mobile IPv6 roaming in networks other than its home has been raised in IETF [4]. It identifies the following information that typically needs to be exchanged between a MN and an AAA Client in the network: MIP Feature Data, EAP Data, Security Key Data, and Embedded Data. It also specifies the use of the new Diameter application in exchanges of the above information between AAA Client and AAAv, between AAAv and AAAh, and between HA and the AAA infrastructure.

Although [4] does not specify any particular mechanism to convey information between the mobile node and the AAA Client, the possibility to use the protocol defined by the IETF PANA WG has been mentioned. On the other hand, the PANA WG has recently identified EAP [6] as the payload for the PANA protocol and carrier for authentication methods [1]. In other words, PANA will carry EAP, which can carry various authentication methods. By the virtue of enabling transport of EAP above IP, any authentication method that can be carried as an EAP method is made available to PANA and hence to any link-layer technology. The PANA WG has assumed a clear division of labor between PANA, EAP and EAP methods. Defining new authentication methods, or deriving/distributing keys is considered outside the scope of PANA. Providing a secure channel that protects EAP and EAP methods against eavesdropping and spoofing is also not an objective of the PANA design.

This implies that apart from carrying the EAP, the PANA protocol will not be able to transport the other MIPv6-related auxiliary information such as MIP Feature Data, Security Key Data, and Embedded Data. Thus, there is no satisfactory prior-art mechanism for MIPv6 roaming in foreign networks and conveying necessary information between MN and AAA Client.

Another drawback of the solution in [4] is that it requires the AAA Client (and AAAv) to understand the authentication method and be aware of the contents of the exchanges (MIP Feature Data, EAP Data, Security Key Data, and Embedded Data) between the MN and the AAAh. It will not be possible to let the AAA Client act as mere pass-through agent, which is one of the major advantages of using EAP (and one of the assumptions for using PANA). Neither will it be possible to apply prior encryption between MN and AAAh (e.g., EAP/TTLS [5]) and the exchanges will be visible over the air interface. Security against eavesdropping, man-in-the-middle and other attacks is likely to be compromised.

These drawbacks and others are overcome by the present invention, according to which an EAP authentication protocol is proposed for combining the terminal mobility of MIPv6 with the user authentication of AAA in a most advantageous way, achieving a complete MIPv6 AAA solution.

Main principles as well as implementation details of the invention will now be described by way of example. General reference is made to the MIPv6 AAA actors and architecture illustrated in Fig. 1.

MIPv6 AAA using PANA and Diameter Combination

A new EAP authentication protocol "EAP/MIPv6" is defined to carry a "MIPv6 authentication method". EAP/MIPv6 should enable negotiation/enforcement of MIPv6 authentication (main goal), as well as support some auxiliary information that facilitate e.g., dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security. PANA is preferably used in carrying EAP/MIPv6 between MN/PAC and PAA/AAA Client. Alternatively, carrier protocols which satisfy EAP requirements on lower layer ordering guarantees as in PPP and [10] may be used to carry EAP/MIPv6 between the MN and AAA Client. Specifically for the 3GPP2 CDMA2000 case, it is possible to carry EAP/MIPv6 between the MN and AAA Client using PPP Data Link Layer protocol encapsulation with protocol field value set to C227 (Hex) for EAP [6].

A preferred embodiment uses Diameter for communication between the AAA client and home server. Beyond the PAA/AAA Client towards and within the AAA infrastructure, Diameter EAP Application [3] is then used to encapsulate EAP/MIPv6 within Diameter, that is, EAP/MIPv6 is carried between the PAA/AAAClient and AAAh. The Diameter protocol is used by AAAh for optional assignment of MIP packet filters via MIP filter rules to the PAA/EP and HA, which correspond to the

filter enforcement points. The Diameter protocol is also used by AAAh for distribution of security keys to PAA for PANA security, and optional signaling of QoS parameters. It should be noted that even though Diameter is the preferred choice, it may sometimes be appropriate to instead use another AAA protocol, such as Radius, with modifications obvious to the man skilled in the art.

Regarding the communication between HA and the AAA infrastructure for exchange of security keys (necessary to establish SA between HA and MN) and accounting, two possibilities are suggested. One possibility is to employ the AAAh-HA interface protocol specified in Diameter MIPv4 Application [2]. Another possibility is to employ a mechanism similar to that currently used in 3GPP2 (i.e. [9]) in conjunction with the IKE [8] framework, to distribute dynamic pre-shared keys between MN and HA. A KeyID is used by the HA to retrieve (or generate) the HA-MN pre-shared key from the AAAh (exactly how this is done is vendor/operator implementation specific, and out of scope of this patent disclosure). The KeyID is generated by the AAAh and upon successful authentication sent to the MN, which in turn sends it to the HA using IKE.

MIPv6 handoffs use a subset of the MIPv6 initiation procedures described above. For the handoff case, since the MN has already been previously assigned a home address and a HA prior to handoff, EAP/MIPv6 would only need to carry information that facilitate MIPv6 authentication, and distribution of security keys between PAC and PAA for PANA security. The MIPv6 authentication which takes place is for authentication to use the newly acquired CoA. As with the MIPv6 initiation case, Diameter protocol is used by AAAh for assignment to PAA/EP of optional MIP packet filters via some kind of MIP filter rule, security keys for PANA security, and optional QoS parameters etc.

When both EAP/AKA for WLAN access authentication, and EAP/MIPv6 have to be carried out, it is proposed to allow single traversal to carry out both simultaneously to

save time and facilitate fast handoff (both AAAv and AAAh are traversed). PANA is used in carrying EAP/MIPv6 between PAC and PAA/AAA Client. PANA can also used for transporting EAP/AKA between PAC and PAA for WLAN access authentication instead of [10]. By carrying multiple EAP sequences in a single PANA sequence, both EAP/AKA for WLAN authentication and EAP/MIPv6 can take place within a single PANA sequence for optimization purposes.

New EAP attributes and exemplary signal flows

In this section, implementation features of the proposed authentication protocol according to the invention will be described. Examples of EAP/MIPv6 protocol details are provided to show the overall flow and viability of concept.

The authentication method of the invention involves new EAP TLVs carrying information that facilitates MIPv6 authentication, dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security.

The following new EAP TLVs are preferably defined under EAP/MIPv6:

MD5 Challenge EAP-TLV attribute
MD5 Response EAP-TLV attribute
MIPv6 Home Address Request EAP-TLV attribute
MIPv6 Home Address Response EAP-TLV attribute
MIPv6 Home Agent Address Request EAP-TLV attribute
MIPv6 Home Agent Address Response EAP-TLV attribute
HA-MN Pre-shared Key Generation Nonce EAP-TLV attribute
IKE KeyID EAP-TLV attribute
HA-MN IPSec SPI EAP-TLV attribute
HA-MN IPSec Key Lifetime EAP-TLV attribute
PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute

By means of (some or all of) these attributes, the EAP protocol can, in addition to the main IPv6 authentication information, carry MIPv6-related auxiliary information, which is a considerable advantage. The MIPv6-related auxiliary information can e.g. comprise requests for dynamic MN home address allocation, dynamic Home Agent allocation, as well as nonces/seeds for creation of necessary security keys.

Different authentication protocols are possible for EAP/MIPv6. A preferred embodiment of the invention proposes implementation through MD5-Challenge authentication, but other protocols also lie within the scope of the invention. The following EAP-TLV attributes are defined for MIPv6 authentication:

i) MD5 Challenge EAP-TLV attribute

This represents the octet string generated randomly by the AAAh and sent to MN for MD5 challenge.

ii) MD5 Response EAP-TLV attribute

This represents the octet string generated as a result of MD5 hash function with the shared secret key between AAAh and MN.

The following EAP-TLV attributes are preferably defined for dynamic MN home address allocation:

iii) MIPv6 Home Address Request EAP-TLV attribute

This represents a request for a dynamically allocated MIPv6 home address for the authenticated MN. It will be requested by the MN to the AAAh when the MN initially requests to be authenticated and given MIPv6 service. This attribute is optional when the MN already has a previously assigned home address, e.g., during MIPv6 handoffs.

iv) MIPv6 Home Address Response EAP-TLV attribute

This represents a dynamic allocated MIPv6 home address for the authenticated MN. It will be notified to the MN from AAAh when the MN, which has requested for one, has been successfully authenticated. This attribute is optional when the MN already has a previously assigned home address, e.g., during MIPv6 handoffs.

The following EAP-TLV attributes are preferably defined for dynamic HA allocation:

v) MIPv6 Home Agent Address Request EAP-TLV attribute

This represents a request for an address of a dynamically allocated HA for the MN when successfully authenticated. It will be requested by the MN to the AAAh when a MN initially requests to be authenticated and given MIPv6 service. As the MIPv6 protocol has a dynamic HA discovery method to allocate the HA, this attribute is optional. This is also the case when the MN already has a previously assigned HA, e.g., during MIPv6 handoffs.

vi) MIPv6 Home Agent Address Response EAP-TLV attribute

This represents an address of a dynamic allocated HA for the authenticated MN. It will be notified to the MN from the AAAh when a MN initially requests to be authenticated and given MIPv6 service. As the MIPv6 protocol has a dynamic home agent discovery method to allocate the home agent, this attribute is optional. This is also the case when the MN already has a previously assigned HA, e.g., during MIPv6 handoffs.

The following EAP-TLV attributes are preferably defined for distribution of security keys between HA and MN:

vii) HA-MN Pre-shared Key Generation Nonce EAP-TLV attribute

This represents the octet string generated randomly by MN as a seed for generating the pre-shared key between HA-MN. The MN can internally generate the HA-MN pre-shared key by using an appropriate hash algorithm on the combination of this nonce

and the shared key between MN and AAAh. This attribute is optional when a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs.

viii) IKE KeyID EAP-TLV attribute

This represents the ID payload defined in [7]. The KeyID is generated by the AAAh and sent to the MN upon successful authentication. The KeyID includes some octets which informs the HA how to retrieve (or generate) the HA-MN pre-shared key from AAAh. This attribute is optional, and would generally not be needed when the MN did not submit a HA-MN pre-shared key generation nonce, i.e., a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs. It is also not needed for the case when the HA-MN pre-shared key is conveyed by the AAAh to the HA via the AAAh-HA interface defined in [2].

ix) HA-MN IPSec SPI EAP-TLV attribute

This represents the Security Parameter Index for IPSec between the HA and MN. This is generated by the HA and informed to the MN for the case when the HA-MN pre-shared key is conveyed by the AAAh to the HA via the AAAh-HA interface defined in [2]. This attribute is optional and is generally not needed when the MN did not submit a HA-MN pre-shared key generation nonce, i.e., a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs. It is also not needed for the case when the AAAh-HA interface defined in [2] is not used.

x) HA-MN IPSec Key Lifetime EAP-TLV attribute

This represents the Key Lifetime for IPSec between the HA and MN. This is generated by the HA and informed to the MN for the case when the HA-MN pre-shared key is conveyed by the AAAh to the HA via the AAAh-HA interface defined in [2]. This attribute is optional and is generally not needed when the MN did not submit a HA-MN pre-shared key generation nonce, i.e., a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs. It is also not needed for the case when the AAAh-HA interface defined in [2] is not used.

Finally, the following EAP-TLV attribute is preferably defined for distribution of security keys between PAC and PAA for PANA security:

xi) PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute

This represents the octet string generated randomly by MN/PAC as a seed for generating the pre-shared key between PAC-PAA. The MN/PAC can internally generate the PAC-PAA pre-shared key by using an appropriate hash algorithm on the combination of this nonce and the shared key between MN and AAAh. This attribute is needed for PANA security.

Preferred schemes for handling MIPv6 initiation and handoff according to the invention are provided in the signaling flow diagrams Figs. 2, 3 and 4. The illustrated examples relate to MIPv6 AAA using a combination of PANA and Diameter as carrier protocols. The flow diagram in Fig. 2 illustrates MIPv6 initiation with use of an AAAh-HA interface according to [2] for exchange of a HA-MN pre-shared key. Another MIPv6 initiation scheme, illustrated in Fig. 3, uses IKE KeyID for exchange of a HA-MN pre-shared key. The signaling flows of Fig. 4 describe MIPv6 handoff in accordance with an examplary embodiment of the invention.

Concluding remarks/Benefits of the invention

A major advantage of the proposed EAP protocol is that it allows EAP to carry MIPv6-related auxiliary information in addition the main MIPv6 authentication information. This auxiliary information may include requests for dynamic MN home address allocation, dynamic Home Agent allocation, as well as nonces/seeds for creation of necessary security keys. The MIPv6-related auxiliary information are exchanged between the Mobile Node and AAAh (home AAA server), and there is no need for intermediaries like AAA Clients and AAAv (visited AAA servers) to understand the information.

Without the proposed solution, i.e. if EAP was not carrying the MIPv6-related auxiliary information, requirements would typically be placed on the carrier protocols like PANA and Diameter to carry this information. This leads to an increased complexity of the carrier protocols and to compromised security (as the information is also picked up by intermediaries AAA Clients and AAAv's).

To sum up, the invention achieves a complete MIPv6 AAA solution for the first time, and does not put unnecessary complexities on carrier protocols. It also enables security of information between the Mobile Node and home AAA server.

Although the invention has been described with reference to specific exemplary embodiments, it also covers equivalents to the described features, as well as modifications and variants obvious to a man skilled in the art.

REFERENCES

[1] Protocol for Carrying Authentication for Network Access (PANA), D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, 2003-4-3

[2] Diameter Mobile IPv4 Application, P. Calhoun, T. Johansson, C. Perkins, 2003-4-29

[3] Diameter Extensible Authentication Protocol (EAP) Application, T. Hiller, G. Zorn, March 2003

[4] Diameter Mobile IPv6 Application, Stefano M. Faccin, Franck Le, Basavaraj Patil, Charles E. Perkins, April 2003

[5] EAP Tunneled TLS Authentication Protocol, Paul Funk, Simon Blake-Wilson, November 2002

[6] PPP Extensible Authentication Protocol (EAP), RFC2284, L. Blunk, J. Vollbrecht, March 1998

[7] Internet Security Association and Key Management Protocol (ISAKMP), RFC2408, D. Maughan, M. Schertler, M. Schneider, J. Turner, November 1998

[8] The Internet Key Exchange (IKE), RFC2409, D. Harkins, D. Carrel, November 1998

[9] 3GPP2 X.P0011 Ver.1.0-9, 3GPP2 Wireless IP Network Standard, February, 2003

[10] IEEE Standard 802.1X, Local and metropolitan area networks – Port-Based Network Access Control

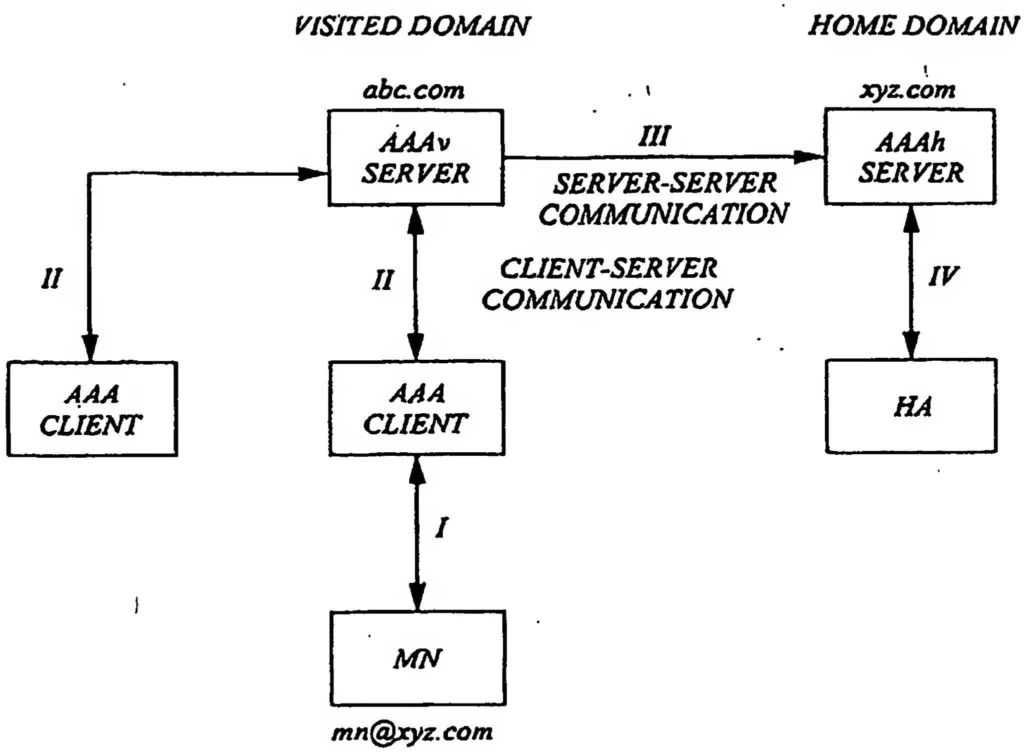
VISITED DOMAIN
HOME DOMAIN
abc.com
xyz.com
AAAv SERVER
III
SERVER-SERVER COMMUNICATION
AAAh SERVER
II
II
CLIENT-SERVER COMMUNICATION
IV
AAA CLIENT
AAA CLIENT
HA
I
MN
mn@xyz.com

FIG. 1

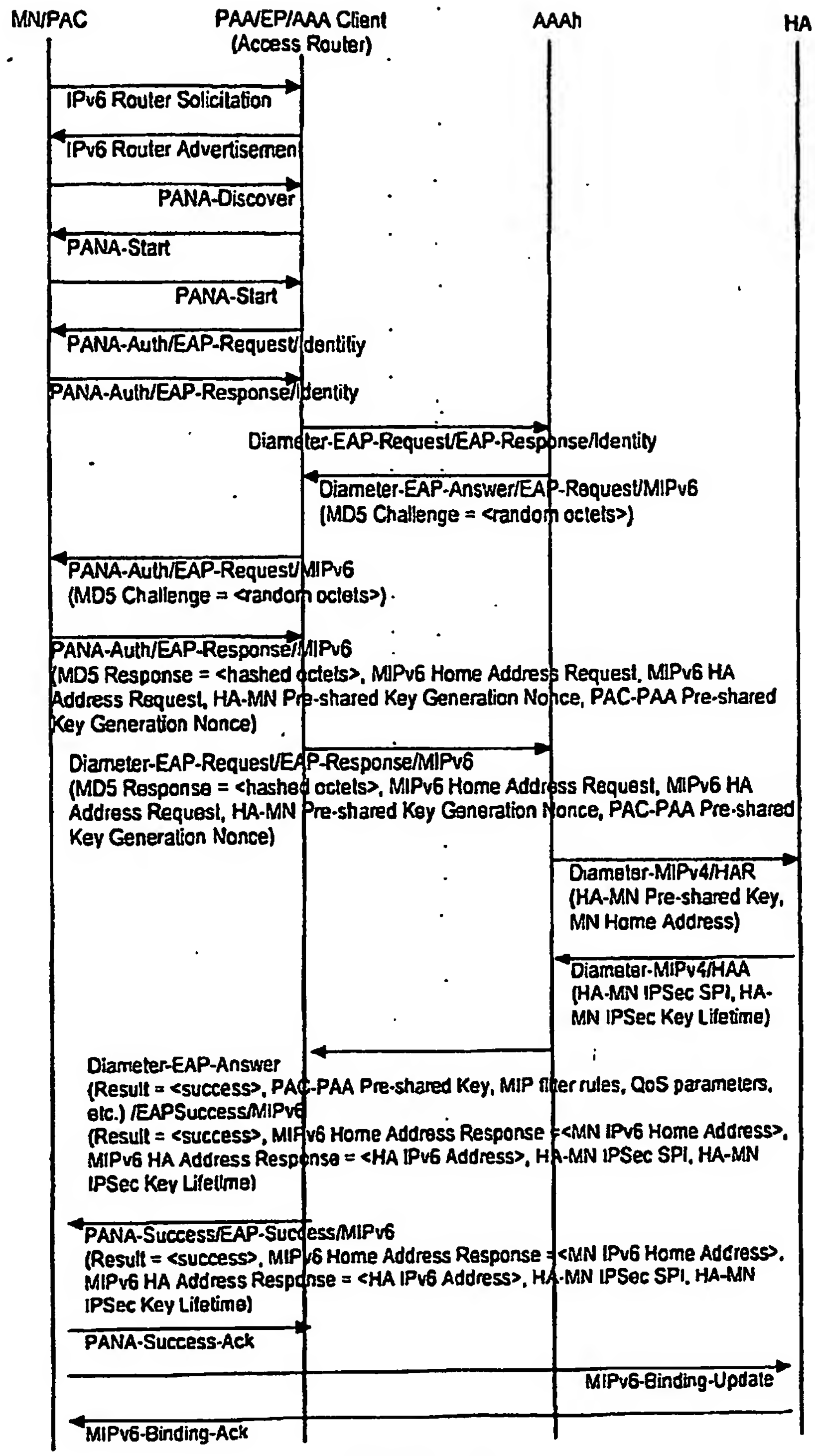
MN/PAC
PAA/EP/AAA Client (Access Router)
AAAh
HA
IPv6 Router Solicitation
IPv6 Router Advertisement
PANA-Discover
PANA-Start
PANA-Start
PANA-Auth/EAP-Request/Identity
PANA-Auth/EAP-Response/Identity
Diameter-EAP-Request/EAP-Response/Identity
Diameter-EAP-Answer/EAP-Request/MIPv6 (MD5 Challenge = <random octets>)
PANA-Auth/EAP-Request/MIPv6 (MD5 Challenge = <random octets>)
PANA-Auth/EAP-Response/MIPv6 (MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Request/EAP-Response/MIPv6 (MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-MIPv4/HAR (HA-MN Pre-shared Key, MN Home Address)
Diameter-MIPv4/HAA (HA-MN IPSec SPI, HA-MN IPSec Key Lifetime)
Diameter-EAP-Answer (Result = <success>, PAC-PAA Pre-shared Key, MIP filter rules, QoS parameters, etc.) /EAPSuccess/MIPv6 (Result = <success>, MIPv6 Home Address Response = <MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, HA-MN IPSec SPI, HA-MN IPSec Key Lifetime)
PANA-Success/EAP-Success/MIPv6 (Result = <success>, MIPv6 Home Address Response = <MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, HA-MN IPSec SPI, HA-MN IPSec Key Lifetime)
PANA-Success-Ack
MIPv6-Binding-Update
MIPv6-Binding-Ack

FIG. 2

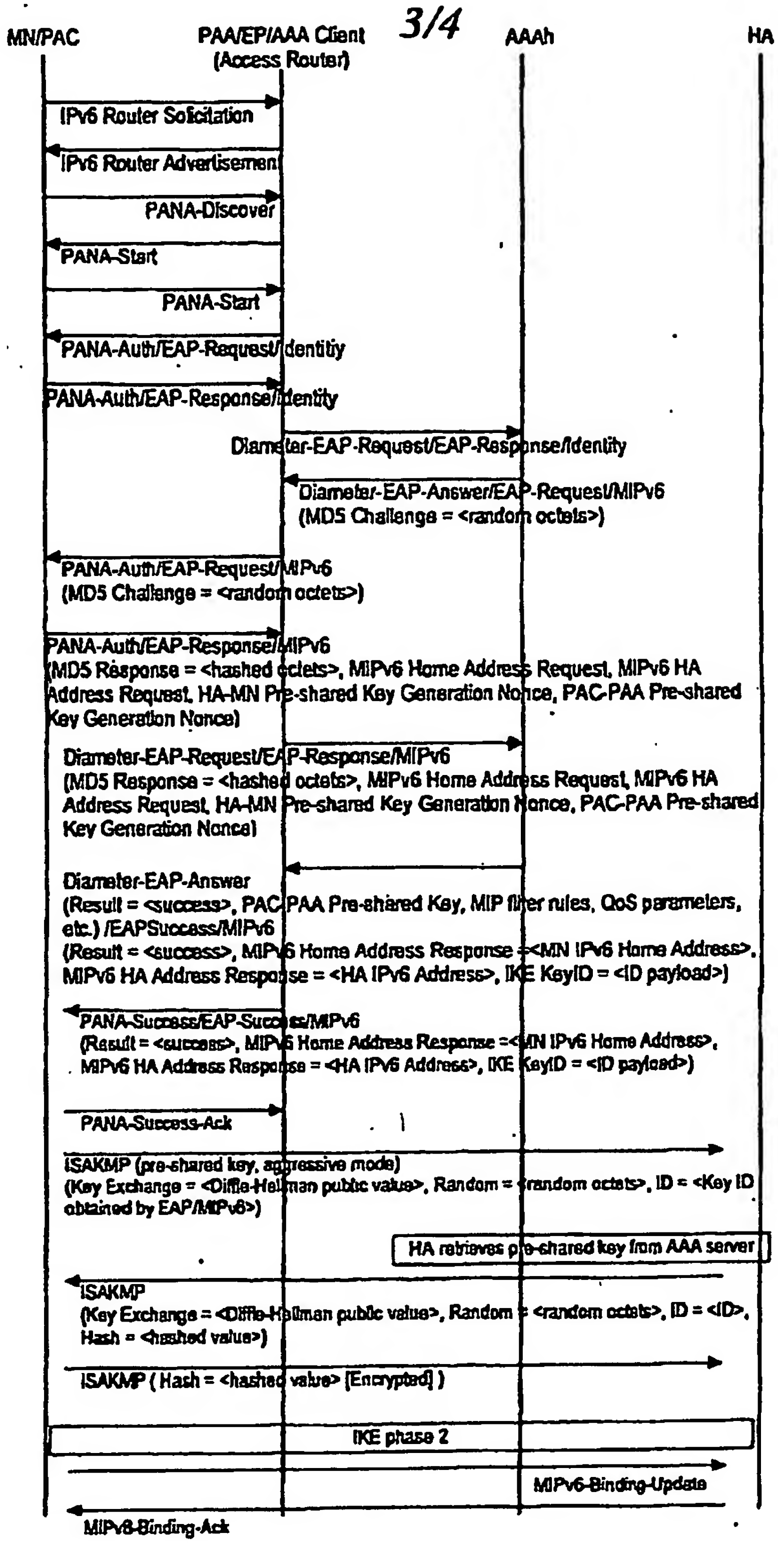
MN/PAC
PAA/EP/AAA Client
(Access Router)
AAAh
HA
IPv6 Router Solicitation
IPv6 Router Advertisement
PANA-Discover
PANA-Start
PANA-Start
PANA-Auth/EAP-Request/Identity
PANA-Auth/EAP-Response/Identity
Diameter-EAP-Request/EAP-Response/Identity
Diameter-EAP-Answer/EAP-Request/MIPv6
(MD5 Challenge = <random octets>)
PANA-Auth/EAP-Request/MIPv6
(MD5 Challenge = <random octets>)
PANA-Auth/EAP-Response/MIPv6
(MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Request/EAP-Response/MIPv6
(MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Answer
(Result = <success>, PAC-PAA Pre-shared Key, MIP filter rules, QoS parameters, etc.) /EAPSuccess/MIPv6
(Result = <success>, MIPv6 Home Address Response = <MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, IKE KeyID = <ID payload>)
PANA-Success/EAP-Success/MIPv6
(Result = <success>, MIPv6 Home Address Response = <MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, IKE KeyID = <ID payload>)
PANA-Success-Ack
ISAKMP (pre-shared key, aggressive mode)
(Key Exchange = <Diffie-Hellman public value>, Random = <random octets>, ID = <Key ID obtained by EAP/MIPv6>)
HA retrieves pre-shared key from AAA server
ISAKMP
(Key Exchange = <Diffie-Hellman public value>, Random = <random octets>, ID = <ID>, Hash = <hashed value>)
ISAKMP (Hash = <hashed value> [Encrypted])
IKE phase 2
MIPv6-Binding-Update
MIPv6-Binding-Ack

FIG. 3

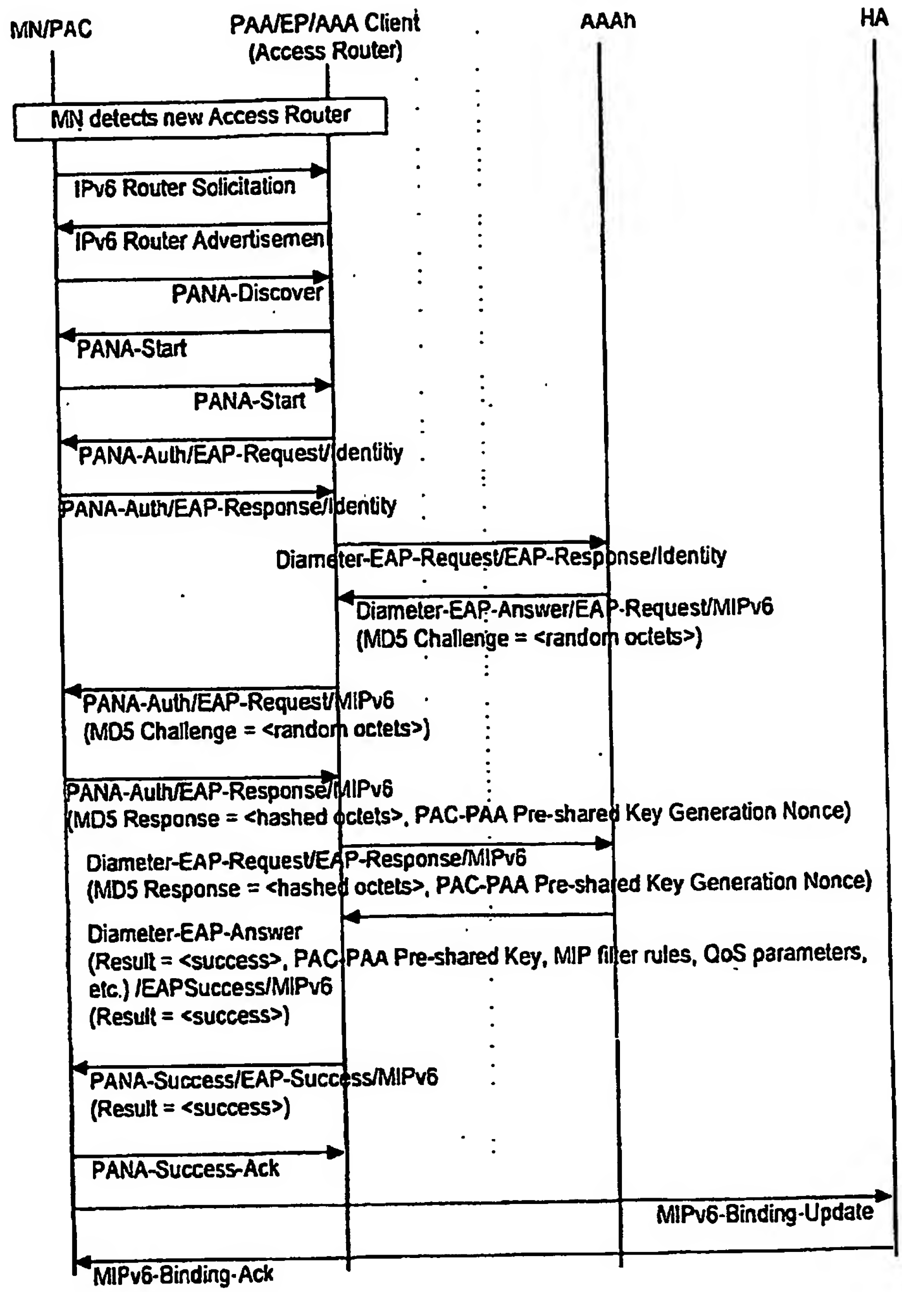
MN/PAC
PAA/EP/AAA Client
(Access Router)
AAAh
HA
MN detects new Access Router
IPv6 Router Solicitation
IPv6 Router Advertisement
PANA-Discover
PANA-Start
PANA-Start
PANA-Auth/EAP-Request/Identity
PANA-Auth/EAP-Response/Identity
Diameter-EAP-Request/EAP-Response/Identity
Diameter-EAP-Answer/EAP-Request/MIPv6
(MD5 Challenge = <random octets>)
PANA-Auth/EAP-Request/MIPv6
(MD5 Challenge = <random octets>)
PANA-Auth/EAP-Response/MIPv6
(MD5 Response = <hashed octets>, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Request/EAP-Response/MIPv6
(MD5 Response = <hashed octets>, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Answer
(Result = <success>, PAC-PAA Pre-shared Key, MIP filter rules, QoS parameters, etc.) /EAPSuccess/MIPv6
(Result = <success>)
PANA-Success/EAP-Success/MIPv6
(Result = <success>)
PANA-Success-Ack
MIPv6-Binding-Update
MIPv6-Binding-Ack

FIG. 4